EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment, which begins on the following page, was given in a telephone interview with Thomas Lees on 5/15/2008.

The application has been amended as follows:

This listing of claims will replace all prior versions and listings of claims in this application:

Listing of the Claims

1. (Previously Presented) A method of impersonating a client to a plurality of servers, comprising:

obtaining by a middle tier server, a common nonce that is created based at least in part upon a pre-nonce contribution from each of a plurality of back-end servers, wherein the common nonce is generated from an entity other than the client that the middle tier server is to impersonate or the plurality of back-end servers that the middle tier server is to interact with on behalf of the client;

receiving by the middle tier server, a request from the client for a transaction with at least one of the plurality of back-end servers;

providing the common nonce from the middle tier server to the client;

receiving the common nonce signed by the client with the client's digital signature at the middle-tier server; and

impersonating the client by the middle tier server interacting with a selected one of the plurality of back-end servers for implementation of the client request on behalf of the client by providing the signed common nonce and the client request from the middle tier server to at least one of the plurality of back-end servers so as to authenticate the client to the plurality of servers for implementation of the client request on behalf of the client.

2. (Canceled)

3. (Previously Presented) The method of Claim 1, wherein obtaining the common nonce comprises:

obtaining the pre-nonce contributions from the plurality of servers;

combining the pre-nonce contributions to provide a single pre-nonce token; and

providing the common nonce based on the pre-nonce token.

4. (Original) The method of Claim 3, wherein the step of providing the common nonce comprises reducing the pre-nonce token to provide the common nonce.

5. (Original) The method of Claim 3, wherein the step of combining the pre-nonce contributions to provide a single pre-nonce token comprises concatenating the pre-nonce contributions.

6. (Original) The method of Claim 4, wherein the step of reducing the pre-nonce token to provide the common nonce comprises the step of hashing the pre-nonce token utilizing a one-way hash function so as to provide the common nonce.

7. (Original) The method of Claim 3, wherein the step of obtaining pre-nonce contributions comprises the steps of:

requesting a pre-nonce contribution from each of the plurality of servers; and receiving the pre-nonce contributions from the plurality of servers.

8. (Original) The method of Claim 7, wherein requesting a pre-nonce contribution comprises sending authenticated requests to the plurality of servers.

9. (Original) The method of Claim 8, further comprising the step of encrypting the authenticated requests sent to the plurality of servers.

10. (Original) The method of Claim 8, wherein the authenticated requests include at least one of an identification of a source of the request, a time stamp and a random number.

11. (Original) The method of Claim 3, wherein the pre-nonce contributions include at least one of an identification of a server of the plurality of servers and a random number.

12. (Original) The method of Claim 3, wherein the pre-nonce contributions are signed with a signature corresponding to a server from which the pre-nonce contribution was obtained, the method further comprising incorporating the signatures in the pre-nonce token.

13. (Original) The method of Claim 3, wherein the pre-nonce contributions are signed with a signature corresponding to a server from which the pre-nonce contribution was obtained, the method further comprising authenticating the signatures of the pre-nonce contributions and rejecting pre-nonce contributions for which the digital signature is not authentic.

14. (Original) The method of Claim 3, further comprising the steps of:

receiving a transaction identification from a trusted server of the plurality of servers; and

associating the transaction identification with the common nonce.

15. (Original) The method of Claim 14, further comprising the step of tracking use of the common nonce based on the transaction identification.

16. (Currently Amended) The method of Claim 3, further comprising the steps of:

associating an expiration ~~line~~ time with a pre-nonce contribution; and

determining if the pre-nonce contribution has expired based on its associated expiration time.

17. (Original) The method of Claim 16, further comprising the steps of:

receiving the common nonce at a server of the plurality of servers;

determining a pre-nonce contribution associated with the received common nonce; and

accepting the received common nonce if the associated pre-nonce contribution has not expired.

18. (Original) The method of Claim 3, wherein at least one of the plurality of servers carries out the steps of:

receiving a client certificate;

determining if the client certificate is trusted; and

indicating that the client is not authenticated if the client certificate is not trusted.

19. (Original) The method of Claim 3, wherein at least one of the plurality of servers carries out the steps of:

receiving the signed common nonce and a client certificate;

determining if the signature of the signed common nonce corresponds to a signature of the client certificate; and

indicating that the client is not authenticated if the signature of the signed common nonce does not correspond to the signature of the client certificate.

20. (Original) The method of Claim 6, wherein at least one of the plurality of servers carries out the steps of:

receiving the signed common nonce, the common nonce and the pre-nonce token;

hashing the received pre-nonce token;

comparing the hashed pre-nonce token to the common nonce;

indicating that the client is not authenticated if the hashed pre-nonce token is different from the common nonce.

21. (Original) The method of Claim 11, wherein at least one of the plurality of servers carries out the steps of:

receiving the pre-nonce token;

determining if the pre-nonce token includes a random number associated with the at least one of the plurality of servers; and

indicating that the client is not authenticated if the pre-nonce token does not include the random number associated with the at least one of the plurality of servers.

22. (Original) The method of Claim 21, wherein at least one of the plurality of servers carries out the steps of:

associating an expiration with the random number associated with the at least one of the plurality of servers; and

indicating that the client is not authenticated if the pre-nonce token does not include a random number associated with the at least one of the plurality of servers which has not expired.

23. (Original) The method of Claim 1, wherein the step of obtaining a common nonce comprises the steps of:

obtaining the common nonce from a party trusted by the middle-tier server and the plurality of servers, the common nonce being signed by the trusted party; and

verifying the signature of the common nonce is the signature of the trusted party.

24. (Original) The method of Claim 23, wherein at least one of the plurality of servers carries out the steps of:

receiving a client certificate;

determining if the client certificate is trusted; and

indicating that the client is not authenticated if the client certificate is not trusted.

25. (Original) The method of Claim 23, wherein at least one of the plurality of servers carries out the steps of:

receiving the signed common nonce and a client certificate;

determining if the signature of the signed common nonce corresponds to a signature of the client certificate; and

indicating that the client is not authenticated if the signature of the signed common nonce does not correspond to the signature of the client certificate.

26. (Canceled)

27. (Canceled)

28. (Canceled)

29. (Canceled)

30. (Canceled)

31. (Canceled)

32. (Canceled)

33. (Previously Presented) The method according to claim 1, further comprising:

combining the pre-nonce contributions from the plurality of back-end servers into a pre-nonce token;

hashing the pre-nonce token by the middle-tier server to generate the common nonce; and

providing the pre-nonce token to the selected one of the plurality of back-end servers; wherein:

the selected back-end server hashes the pre-nonce token using the same hashing technique used by the middle-tier server and compares it to the verified common nonce thus authenticating both the client and the middle-tier server the selected back-end server.

The following is an examiner's statement of reasons for allowance: While the prior art, namely Kaliski, Jr., provides teachings of a "common nonce" comprised of nonces from a plurality of servers, the prior art fails to teach or suggest the specific combination of limitations as claimed, which recites obtaining by a middle tier server, a common nonce that is created based at least in part upon a pre-nonce contribution from each of a plurality of back-end servers, wherein the common nonce is generated from an entity other than the client or the plurality of back-end servers, providing the common nonce from the middle tier server to the client,

receiving the common nonce signed by the client at the middle tier server, and impersonating the client by the middle tier server.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Matthew T Henning/
Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131